Bezpieczeństwo informacji - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Bezpieczeństwo informacji
Kod przedmiotu	06.9-WM-IBezp-P-52_15gen
Wydział	Wydział Mechaniczny
Kierunek	Inżynieria bezpieczeństwa
Profil	ogólnoakademicki
Rodzaj studiów	pierwszego stopnia z tyt. inżyniera
Semestr rozpoczęcia	semestr zimowy 2016/2017

Informacje o przedmiocie

Semestr	6
Liczba punktów ECTS do zdobycia	2
Typ przedmiotu	obowiązkowy
Język nauczania	polski
Sylabus opracował	• dr hab. Eunika Baron-Polańczyk, prof. UZ • dr Aneta Klementowska • dr Maria Agnieszka Paszkowicz

Formy zajęć

Forma zajęć	Liczba godzin w semestrze (stacjonarne)	Liczba godzin w tygodniu (stacjonarne)	Liczba godzin w semestrze (niestacjonarne)	Liczba godzin w tygodniu (niestacjonarne)	Forma zaliczenia
Wykład	15	1	9	0,6	Zaliczenie na ocenę
Ćwiczenia	15	1	9	0,6	Zaliczenie na ocenę

Cel przedmiotu

Zapoznanie studentów z działaniem oraz eksploatacją systemów podnoszących bezpieczeństwo informacji. Zdobycie umiejętności posługiwania się podstawowymi programami do szyfrowania dokumentów oraz szyfrowania transmisji w sieciach komputerowych.

Wymagania wstępne

Brak wymagań wstępnych.

Zakres tematyczny

Terminologia i klasyfikacja tajemnic. Podstawy prawne w ochronie informacji, tajemnice prawnie chronione. Podstawowe moduły w zarządzaniu bezpieczeństwem informacji. Polityka bezpieczeństwa informacji. Wytwarzanie, przetwarzanie i przechowywanie dokumentów w systemach teleinformatycznych. Zasady udostępniania informacji – zagrożenia i mankamenty. Zabezpieczenia i wymagania w zakresie ochrony informacji. Administracyjne, techniczne i fizyczne bezpieczeństwo danych.

Metody kształcenia

Zajęcia laboratoryjne, ćwiczenia praktyczne, dyskusja problemowa.

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć

Opis efektu	Symboleefektów	Metody weryfikacji	Forma zajęć
Zna i rozumie podstawowe pojęcia i zasady z zakresu ochrony własności przemysłowej i prawa autorskiego. Zna podstawowe metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu prostych zadań dotyczących eksploatacji systemów podnoszących bezpieczeństwo informacji w Inżynierii Bezpieczeństwa. Ma podstawową wiedzę niezbędną do rozumienia społecznych, ekonomicznych, prawnych i innych pozatechnicznych uwarunkowań działalności inżynierskiej. Prawidłowo posługuje się systemami normatywnymi oraz wybranymi normami i regułami (prawnymi, zawodowymi, moralnymi) w celu rozwiązania konkretnego zadania z zakresu dziedzin nauki i dyscyplin naukowych, właściwych dla Inżynierii Bezpieczeństwa. Potrafi planować i przeprowadzać eksperymenty, w tym pomiary i symulacje komputerowe, interpretować uzyskane wyniki i wyciągać wnioski warunkujące bezpieczeństwo informacji. Potrafi wykorzystać do formułowania i rozwiązywania zadań inżynierskich metody analityczne, symulacyjne oraz eksperymentalne zabezpieczające informacje. Potrafi — przy formułowaniu i rozwiązywaniu zadań inżynierskich — dostrzegać ich aspekty systemowe i pozatechniczne związane z eksploatacją systemów podnoszących bezpieczeństwo informacji. Potrafi dokonać krytycznej analizy sposobu funkcjonowania i ocenić — zwłaszcza w powiązaniu ze studiowanym kierunkiem studiów — istniejące rozwiązania techniczne wpływające na bezpieczeństwo informacji. Potrafi ocenić przydatność rutynowych metod i narzędzi służących do szyfrowania dokumentów oraz szyfrowania transmisji w sieciach komputerowych charakterystycznych dla studiowanego kierunku studiów oraz wybrać i zastosować właściwą metodę i narzędzia. Potrafi — zgodnie z zadaną specyfikacją — zaprojektować oraz zrealizować proste projekty zabezpieczeń informacji typowych dla studiowanego kierunku studiów, używając właściwych metod, technik i narzędzi. Ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżynierskiej, w tym jej wpływu na środowisko, i związanej z tym odpowiedzialności za podejmowane decyzje w zakresie bezpieczeństwa informacji. Potrafi myśleć i działać w sposób przedsiębiorczy. Rozumie potrzebę uczenia się przez całe życie.	• K_W09 • K_U09 • K_K01 • K_K02 • K_K06	• aktywność w trakcie zajęć • kolokwium • sprawdzian	• Wykład • Ćwiczenia

Warunki zaliczenia

Zaliczenie na ocenę ćwiczeń odbywa się na podstawie ocenionych projektów i sprawdzianów. Wykład zaliczany jest w pisemnego sprawdzianu. Ocena wypadkowa ustalana jest na podstawie średniej z ocen z ćwiczeń i wykładu z jednakową wagą.

Literatura podstawowa

Garfinkel S., Spafford G., *Bezpieczeństwo w Unixie i Interne*cie, Wyd. RM, Warszawa 2003.

Frisch A., *Unix. Administracja systemu,* Wyd. RM, Warszawa 2003.

ISO/IEC 27001 – norma międzynarodowa standaryzująca systemy zarządzania bezpieczeństwem informacji.

Literatura uzupełniająca

Stokłosa J., Bliski T., Pankowski T., *Bezpieczeństwo danych w systemach informatycznych*, PWN, Warszawa 2001.

Cheswick W., *Firewalle i bezpieczeństwo w sieci*, Helion, Gliwice 2003.

Uwagi

Zmodyfikowane przez dr hab. Eunika Baron-Polańczyk, prof. UZ (ostatnia modyfikacja: 13-09-2016 12:04)